# Platoon-Based Approach for VANET Communication and Management

**Objective**: To develop a platoon-based communication system that addresses VANET (Vehicular Ad-hoc Network) concerns by reducing the load on roadside units and ensuring safe and efficient inter-platoon communications.

Intra-Platoon Communication (Not really a novelty feature)

* Overview: Intra-platoon communication is designed to manage commands and maneuvers within a single platoon. Each platoon consists of multiple vehicles, with a designated leader vehicle responsible for executing commands and verifying actions.
* Command Execution: When a vehicle within the platoon wants to execute a command or perform a maneuver (e.g., tailgating), it communicates with the leader. The leader processes and broadcasts the command to ensure synchronized execution across the platoon.
* Designation of Vehicles: During the joining process, the leader randomly designates two vehicles with trust scores above a specific threshold to positions at the front and back of the platoon. These vehicles play critical roles in managing inter-platoon communications and ensuring platoon integrity.
* Rest is similar as in Thesis

Inter-Platoon Communication (A proper novelty feature)

* Scenario Management: In the event of an approaching Law Enforcement Agency (LEA) vehicle traveling at high speed, the system is designed to allow safe and efficient passage without blocking the LEA vehicle.
* LEA Vehicle Identification: The LEA vehicle is treated as a special entity that transmits a distinct signal, similar to a conventional siren. This signal is immediately recognized by the platoon.
* Leader’s Role: Upon detecting the LEA signal, the leader of the platoon communicates with the designated front and rear vehicles. The leader then executes a command for the entire platoon to slow down and move aside, allowing the LEA vehicle to pass.
* Verification Process: After the LEA vehicle has passed, the rear-designated vehicle verifies the completion of the maneuver. This verification process ensures that all actions are properly executed and documented.
* Rest is properly explained below.

Event Logging and Trust Score Management

* Event Logging: Upon completion of the maneuver, the event is recorded as a transaction on a blockchain. This provides an immutable record of the event, contributing to the transparency and accountability of the system.
* Trust Score Adjustments: If the LEA signal is later determined to be false, the trust score of the initiating vehicle is reduced. This mechanism helps maintain the integrity of the platoon by discouraging false signals and encouraging responsible behavior.

Additional Use Cases

* Accident Scenarios: The system can also handle accident scenarios where immediate action is required. The platoon can disperse and send signals to nearby platoons to ensure coordinated responses to emergencies.
* Inter-Platoon Maneuvers: In cases where a vehicle needs to speed up and pass the platoon, the rear-designated vehicle sends a signal to the leader. The leader coordinates the platoon to disperse in a timely manner, allowing the maneuvering vehicle to pass safely.

# Inter-Platoon Communication Protocol

**Intro:** This protocol is designed to facilitate communication between platoon leaders of different platoons with minimal computational overhead, especially in critical situations where time constraints are significant. The protocol ensures quick decision-making, secure information exchange, and coordinated actions among platoons without burdening the system.

**Protocol Steps:**

**1. Platoon Leader Identification and Grouping:**

* **Leader Beaconing** involves each platoon leader periodically sending out a "Leader Beacon" message. This message includes the leader's unique ID, their current status (like speed and position), and the platoon's overall trust score, which reflects the platoon's reliability and performance.
* **Dynamic Grouping** refers to the automatic formation of an Inter-Platoon Communication Group when nearby platoon leaders detect each other's beacons. This temporary communication group adjusts as platoons move in and out of the area, allowing for real-time coordination and communication.
* In practice, these mechanisms help manage traffic in a network of vehicles. For instance, when platoons come close on a highway, Leader Beaconing allows them to share their status, and Dynamic Grouping enables them to form a communication network to synchronize their movements, improving traffic flow and safety.

**2. Command Exchange Request:**

* When a critical situation arises (e.g., obstacle detection, sudden route change, or emergency stop), the affected platoon leader sends a "Command Exchange Request" to all platoon leaders in the Communication Grp. This acts as a trigger event.
* A **Command Exchange Request** is a critical message sent by a platoon leader during emergencies like detecting an obstacle or needing an urgent route change. It includes details about the situation, the specific action needed, the leader’s ID, a timestamp indicating when the request was made, and a cryptographic signature to ensure its authenticity.
* Then request validation is done.Upon receiving a CER, each platoon leader verifies the authenticity and urgency of the request using pre-shared keys and a timestamp. This ensures that only legitimate and timely requests are processed.
* To ensure security, the **pre-shared key**—a secret known only to the platoon leaders—is used to verify the request. This key encrypts or authenticates the CER, preventing unauthorized access. The **timestamp** helps validate that the request is current and prevents old or outdated instructions from causing confusion. In a certificateless cryptographic scheme, these elements work together to secure communications without relying on traditional certificates, ensuring that only legitimate, timely requests are acted upon.

**3. Distributed Command Evaluation:**

* The platoon leader proposing the Cmd Exchange Request includes a proposed command (e.g., stop, reroute, speed adjustment) that it plans to issue within its platoon.
* Other platoon leaders in the grp quickly evaluate the proposed command based on their sensor data, current status, and knowledge of the environment. This evaluation is conducted in parallel to reduce time.
* Each platoon leader sends a concise "Consensus Feedback" to the originating leader, indicating agreement, disagreement, or suggestions for command modification.

**4. Consensus Command Issuance:**

* The originating platoon leader aggregates the feedbacks from the comm. grp. If a majority agree, the command is issued. If there are disagreements, the leader considers alternative suggestions and reissues a modified CER if necessary.
* Once a consensus is reached, the command is immediately executed by all involved platoons, ensuring synchronized action across the platoons.
* If no consensus is reached within a critical time window, the originating leader may issue the command based on its best judgment, but with a "Caution Flag" (CF) attached, signaling potential risk.

**5. Trust and Accountability Mechanism:**

* Once command is executed the transactions and performance are logged in the all of the platoon’s members which are in the grp.
* Performance logs are reviewed by a Trusting Authority (TA). The TA assesses these logs and updates the trust scores of each platoon. If a platoon repeatedly fails to follow commands or poses risks, it might be flagged as "Restricted," and its leader could be removed from the Comm. Grp.
* In case a leader’s trust score drops below a threshold, a new leader election process is initiated within the platoon, and the new leader joins the IPCG.

**6. Critical Situation Override:**

* In extreme emergencies (e.g., collision imminent, critical failure), any platoon leader can invoke a "Critical Situation Override", thus bypassing the consensus process.
* The leader broadcasts an emergency command to all inter-platoon comm. grp members, who have to follow it immediately.
* After the emergency, the grp conducts a review to determine if the override was justified and adjusts trust scores accordingly.

**Key Features:** The protocol is designed with low computation overhead, using straightforward consensus and trust mechanisms to keep processing efficient and decision-making swift. Its scalability ensures that as more platoons join the network, the system can grow seamlessly without overloading communication channels. Security and trust are integral, with features like pre-shared keys, timestamps, and regular trust updates to ensure that only credible leaders are involved in decision-making. Despite its structured approach, the protocol offers autonomy and flexibility, allowing leaders to make quick decisions in critical situations while still promoting consensus among platoons.

**Regular Situations**

* **Traditional Scheme (Centralized or Less Efficient):**
  + **Time Complexity:** O(N^2) for communication and consensus if every leader has to communicate with every other leader.
  + **Space Complexity:** O(N^2) due to the need to store all pairwise communication and feedback.
* **Our Scheme:**
  + **Time Complexity:** O(N) for beaconing, command exchange, and consensus processes.
  + **Space Complexity:** O(N) for storing leader information and feedback.

**Reduction Factor:**

* **Computation Time Reduction:**
  + Traditional scheme: O(N^2) for communication.
  + IPCP scheme: O(N) for communication.
  + **Approximate Reduction Factor:** N^2/N = N. For large N, IPCP can reduce computation time by a factor of NNN.
* **Cost Reduction:**
  + **Computation Cost:** Given the reduced time complexity and parallel processing, the cost associated with computation (in terms of CPU cycles) can be significantly reduced. For large platoon sizes, this reduction can be substantial, potentially up to an N-fold decrease in computation cost.

**Emergency Situations**

* **Traditional Scheme (Centralized or Less Efficient):**
  + **Time Complexity:** O(N^2) due to the need for rapid communication and decision-making among all leaders in an emergency.
  + **Space Complexity:** O(N^2) for storing all emergency commands and responses.
* **Our Scheme:**
  + **Time Complexity:** O(N) for broadcasting emergency commands and executing them based on the consensus.
  + **Space Complexity:** O(N) for handling emergency commands and responses.

**Reduction Factor:**

* **Computation Time Reduction:**
  + Traditional scheme: O(N^2) for emergency communication.
  + IPCP scheme: O(N) for emergency communication.
  + **Approximate Reduction Factor:** N^2/N = N. In emergency situations, IPCP can reduce computation time by a factor of N, similar to regular situations.
* **Cost Reduction:**
  + **Computation Cost:** The cost can be reduced by a factor of N due to lower time complexity and more efficient handling of emergency situations, allowing for quicker response with less computational overhead.

**Summary:**

Implementing IPCP can lead to a significant reduction in both computation time and cost, especially as the number of platoon leaders increases. The reduction factor can be approximated as N, where N is the number of platoon leaders. This is particularly beneficial in both regular and emergency situations, making IPCP a highly efficient protocol for managing platoon communications and decision-making.

**Evaluation of the Protocol**

| **Aspect** | **Rating** | **Comments** |
| --- | --- | --- |
| **Security** | High | - **Leader Beaconing** uses unique IDs, current status, and trust scores to ensure accurate leader identification. - **Command Exchange Request** includes cryptographic signatures and pre-shared keys for validation. - **Consensus Feedback** is used to ensure command agreement and integrity. - **Critical Situation Override** ensures immediate response in emergencies. |
| **Scalability** | High | - **Dynamic Grouping** allows the protocol to adapt to changes in platoon formations. - **Distributed Command Evaluation** and **Consensus Command Issuance** ensure that the protocol scales effectively with the number of platoons. |
| **Certificateless Cryptographic Scheme** | High | - Uses pre-shared keys and timestamps to ensure secure communication without relying on traditional certificates. - Reduces overhead associated with certificate management while maintaining robust security. |
| **Computation Time** | Moderate | - **Leader Beaconing** and **Dynamic Grouping** are efficient. - **Command Exchange Request** and **Distributed Command Evaluation** could be intensive, but parallel processing helps. - Overall time complexity is linear with respect to the number of platoons (O(N)). |
| **Computation Cost** | Moderate | - **Leader Beaconing** and **Distributed Command Evaluation** involve some computational resources, but are manageable. - Cost increases with the number of platoons, but efficient processes help to keep it reasonable. |
| **Potential Use of Blockchain** | High | - **Blockchain** could enhance **Trust and Accountability Mechanism** by providing immutable logs of performance and command execution. - Blockchain could further secure the consensus process and leader election. |

**Tabular Comparison with Traditional Schemes**

| **Aspect** | **Traditional Schemes** | **IPCP** |
| --- | --- | --- |
| **Security** | - Often relies on centralized control and traditional certificates. - Vulnerable to single points of failure. | - Decentralized with cryptographic measures. - Enhanced security through pre-shared keys and timestamps. |
| **Scalability** | - Centralized systems struggle with scalability. - Higher communication and processing overhead as number of leaders grows. | - Dynamic Grouping and distributed evaluation allow for efficient scaling. - Linear scalability with platoon size. |
| **Certificateless Cryptographic Scheme** | - Typically relies on traditional certificates, adding overhead. | - Uses certificateless cryptography, reducing complexity and overhead while maintaining security. |
| **Computation Time** | - Often high due to centralized coordination and communication overhead. - Quadratic or worse complexity. | - More efficient with linear time complexity. - Parallel processing of commands and feedback. |
| **Computation Cost** | - Higher due to extensive communication and processing requirements. - Increased with scale. | - Lower due to efficient communication and processing. - Cost scales linearly with platoon size. |
| **Potential Use of Blockchain** | - Not typically utilized, leading to potential issues with trust and accountability. | - Blockchain could be integrated to enhance trust, accountability, and command validation. |